CSIRT Requirements for Situational Awareness

INTRODUCTION

Situational Awareness in the Context of Computer Security

The term *situational awareness* comes from the field of aviation. It describes the process of evaluating all the different environmental data around you and using it to make decisions. In the area of computer security, it refers to collecting the information around you, understanding how the information relates to and impacts your organization or constituency, and then, at the highest level, using this information to predict future activity. Situational awareness provides a context for decision making and specifically the context within which organizations prevent, detect, and respond to computer security threats and risks.

In military strategy this is very similar to the "OODA Loop," which refers to observe, orient, decide, and act (OODA). The premise of OODA is that all decisions happen within the cycle of observe, orient, decide and act (see http://www.tibco.com/blog/2013/07/11/john-boyd-the-ooda-loop-and-near-real-time-analytics/). With regard to CSIRTs, situational awareness provides mechanisms for observing the environment and orienting (or filtering) the information collected based on needs and perspective, and then using this information to decide and act.

Military, emergency response, and some Computer Security Incident Response Teams (CSIRTs) organizations also talk about situational awareness in similar terms as a common operational picture (COP). A COP synthesizes and displays relevant incident information to understand what is happening where. All pieces of information from multiple sources are integrated to provide that understanding. When that information is shared, then a common understanding is achieved by participants.

For CSIRTs, information assessed and correlated can include but not be limited to incident and vulnerability reports, network traffic, system logging, threat assessments and intelligence along with local and world news and current events.

Situational awareness is an ever-evolving picture of the surrounding environment in which daily activity is occurring. By including economic, social, political, and geographic events into the assessment process, events that by themselves may not seem noteworthy can be identified as suspicious or even malicious. This context in which to observe, assess, and correlate events and information is required at the local or internal organizational level (organizational events such as layoffs, special high profile events, etc.) and also at the external or national or world level (meetings of international organizations in the limelight or under scrutiny such as the World Bank, Olympics, etc.).

CONTACTS

Richard Caralli
Technical Director –
Cyber Security Solutions
412-268-9006
rcaralli@cert.org

Roman Danyliw
Technical Director –
Cyber Threat & Vulnerability
Analysis
412-268-5466
rdd@cert.org

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

James Spencer
CERT Business Manager
703-908-2182
jlspencer@sei.cmu.edu

Software Engineering Institute
4301 Wilson Blvd.
Suite 200
Arlington, VA 22203

www.sei.cmu.edu
www.cert.org

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **25 JAN 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE
CSIRT Requirements for Situational Awareness Tools

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Murray /Robin M. Ruefle M.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon Software Engineering Institute, 4500 Fifth Ave, Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**13**	

Overview of Document

This document provides a high-level view (including corresponding references where available) that describes some of the requirements that the CERT® Division of the Software Engineering Institute at Carnegie Mellon University believes should be considered when developing any type of situational awareness tool.[1] Three aspects related to this topic are discussed:

1. types of situational awareness services currently being provided
2. specific requirements for CSIRTs
3. considerations and constraints

There is also a bibliography in Appendix B that has a collection of articles on or related to situational awareness and computer network defense. Some of these articles are called out later in this document.

Specifically, Skopik, Ma, Smith, and Bleier, in their paper *Designing a Cyber Attack Information System for National Situational Awareness* (Skopik et al. 2012), define an architecture and framework for building a national situational awareness system they call CAIS. This system may have components that would also fit an Internet Climate and Weather service, if that service is to be based on data collection from logs and network traffic of various systems as well as contextual analysis.

TYPES OF CURRENT SITUATIONAL AWARENESS SERVICES

There are various organizations currently supplying different types of situational awareness information that can be used by CSIRTs. Some organizations provide CSIRTs information about malicious activity they see on their own sensor networks that come from other CSIRT constituent systems. For example CERT.br, the Brazilian National CSIRT, has its own honeypot project that collects information about attacks against the honeypots and reports to requesting CSIRTs in other countries, when they see systems in the other CSIRT's country or constituency performing the attack or being a victim of the attack. Other organizations provide for-fee services and provide threat intelligence reports and ongoing briefings. This is mainly done by managed security providers such as Dell SecureWorks, Deloitte, or similar providers. Some organizations provide public reports on threats and risks on a periodic basis, such as Symantec, Verizon, Ponemon Institute, and others. Even other organizations provide information across trusted partners, usually in a non-public fashion. Some of these groups include:

- Information Sharing and Analysis Centers (ISACs)
- the DHS Cybersecurity Information Sharing and Collaboration Program (CISCP) program which shares information with critical infrastructures owners and operators
- the Defense Industrial Base Collaborative Information Sharing Environment (DCISE) which shares information between Defense Industrial Base (DIB) Partners and U.S. Government Stakeholders[2]
- Defense Security Information Exchange (DSIE) whose members share intelligence on cyber related attacks[3]

[1] The SEI/CERT has not collected inputs from external organizations for this paper and, as such, the content here reflects the insights and opinion of CERT technical staff.

[2] For more information on DCISE, see https://www.dc3.mil/dib-cybersecurity/about-dcise

[3] For more information on DSIE, see http://www.whitehouse.gov/files/documents/cyber/Defense%20Security%20Information%20Exchange%20-%20DSIE%20summary%20-%20William%20Ennis.pdf

There are many different models of information sharing that exist and many different organizations that participate in varied manners. The types of organizations involved and the type of information being shared changes dynamically. Appendix A gives some examples of some of the types of data that that is being shared along with related projects dealing with information exchange or formats.

CSIRT REQUIREMENTS FOR SITUATIONAL AWARENESS TOOLS

Below are 14 requirements or features that would be beneficial to any situational awareness service that will be providing information to multiple, diverse CSIRTs. They are not listed in priority order, and some have overlapping components. Many of these requirements might be considered as components of any Internet Weather/Climate service. Others relate to how the service might be designed or implemented.

Requirement 1: Gap Analysis of Current Services

Because so many different services are currently available, before any type of situational tools or services are provided, a good review of existing services should be done, followed by a gap analysis to identify where services are still needed or are not addressed adequately. One idea might also be to hold an industry day for vendors and providers of such services to hear what they currently provide and are planning for the future and to see where economies of scale or collaborations could be achieved.

Requirement 2: Establish a Resource Library Portal with Knowledge Management Document Searching Capability

Such a site will bring together existing data already being collected and create a resource library for searching and correlation. As part of any tool, it would be useful to have a resource library that provides and maintains historical data along with current predictions. Links to all threat and intelligence reports, as well as links to vulnerability and incident summaries, should be included. A strong query capability would need to be developed, so that a CSIRT analyst could put in terms and get back everything that was known about that particular topic. Filtering and advanced querying capability would also be needed to when more specific information was needed.

Requirement 3: Customizable Feeds and Alerts Related to Your Region, Infrastructure, and Internal Environment

The service should provide the ability to customize the feeds and data received by the CSIRT and to fine tune the data to match topics of interest or incidents and vulnerabilities related to similar infrastructures, business missions, and lines of business. For example, the CSIRT should be able to get customized information about attacks against specific operating systems, applications, or even sectors. Another, more important capability would be to receive information relevant to your particular part of the world, regionally and then locally, just like the regular weather stations and channels provide. Along with a description of notable activity that is being seen, information on the type of organizations, sectors (e.g., banking/finance, government, general), or geographical regions that are being affected is needed. Participating organizations should be able to filter information and also set alerts for particular types of information

Requirement 4: Ability to Integrate Organizational Information and Correlate with Provided Feeds

Having the ability for a participating CSIRT to be able to take their own private data and correlate it with the information provided through the program service would be an additional benefit. A method would need developed so that the information they are providing is not shared with anyone else. Such a capability would really allow a CSIRT to take advantage of what is being provided in a common way and use it based on their unique needs.

Requirement 5: Ability to Automate Actions for the CSIRTs Internal Environment

This capability would allow the CSIRT organization to create APIs to take incoming trusted information from the service and filter it through their own established criteria to create automatic actions in their infrastructure. Such actions could include implementing blocks, adding IPs, domains or sites to blacklists, adding signatures for detection in IDS, etc. Such automation could also be set up to originate from the CSIRT organization, so for example – if an alert was received on their IDS or if a specific type of malware was seen or a particular incident reported, then an automatic search of the service could be set up so that all the information known about that particular item would be presented to the CSIRT analyst.

Requirement 6: Secure Information Sharing Between Vetted CSIRTs

Although public information can be very useful to CSIRTs for general trend and indicator information, often there needs to be more detailed discussion of the actual activity, analysis, root cause, and remediation than is possible in a public setting. There must be a way to have secure discussions and information sharing, through protected channels and only for vetted CSIRTs. It would also be helpful to have some identification of others who have expertise in various analysis, detection, or mitigation techniques and tools that a CSIRT could go to for help or advice.

Requirement 7: Ability to Get Feed of Known Fixes

This is a gap area that is not being adequately addressed for all participants. This could also tie into the historical resource library.

Requirement 8: Real-World News Feeds

This should include not only specific cybersecurity-related activity but also social, political, economic, and regional news feeds. This information would be specifically related to ongoing critical infrastructure activities, where international organizations are meeting, where decision makers are gathering for conferences, summits, sports or cultural activities, and similar information that can be used to provide context to network and system activities being seen.

Requirement 9: Continuous Information Collection, Correlation, and Analysis

Very often, trend analysis is only done on a periodic basis, perhaps every quarter, six months, or year (like the Symantec Internet Threat Reports or the CyberCrime Surveys). If some type of continuous trend analysis could be done on current data, so that you did not have to wait for six months, this would be extremely beneficial. Many CSIRTs do not have the expertise, resources, or data to do such continuous analysis. Specifically, the ability to quickly understand historical and contextual information surrounding some new report is important. For example, a new incident is reported from the constituency, prior to that report going to an analyst for handling, it could be correlated against information available in the SA tool, and the complete picture provided to the analyst.

Requirement 10: Assistance in Performing Impact Analysis

In order to react in a timely manner, CSIRTs need to know what impact threat data has (or would have) on their own IT environment. Because of how generally similar the components of most organizations infrastructure has become, many organizations are taking information directly from trusted feeds and implementing detection or mitigation strategies from those feeds, or at least set alerts based on the feeds and then investigating when the alert executes. However in unique situations or with very new unknown threats, CSIRTs may not have the expertise or resources to determine the impact. As part of this service, having experts who can help CSIRTs determine the impact, either by working with them or doing the analysis for them, would be highly beneficial.

Metrics can provide some help in determining this impact. Perhaps some type of system similar to how vulnerability information is analyzed with the Common Vulnerability Scoring System (CVSS) could be developed, where local information is able to be input to help understand the impact to the local organization. In the area of vulnerabilities, teams often evaluate the base and temporal CVSS scores to prioritize their patching needs. Some CSIRT teams may even calculate their own environmental CVSS score for each vulnerability received, but this is rare because the cost of data gathering to perform another calculation can be high. Tools to reduce the cost of data gathering at the local level are often requested. Other analysis has also shown that the CVSS metric alone is not enough to make an informed patching decision. Other metrics and analysis of trends are also needed. For example, Roytman found that having bulk data on which vulnerabilities were being used in live security breaches was more informative than a risk score (Roytman 2013).

Requirement 11: Collect Root Cause Information and Long-Term Analysis

In order to improve, CSIRTs need to understand where weaknesses in the infrastructure occur and where malicious actors are taking advantage of these weaknesses. Any new tool for situational awareness should not only be focused on current attacks, but should also strive to collect lessons learned and after-the-fact analysis so that a better understanding of what happened and how it could be stopped or prevented can be identified. Having participants submit these long-term analysis reports along with more immediate root cause data can help organizations plan security defenses, see where there are inefficiencies existing and efficiencies to be gained, and determine how to make security investments with tight funds to get the greatest return.

Requirement 12: Include Information on Emerging Trends

In order to improve, CSIRTs want to know what changes are being seen in not only attacks, but technologies, mitigations, and even process improvement. The service should ensure this kind of information is collected, shared, and placed into the resource library. It should perhaps develop some business scenario simulations, where organizations and CSIRTs can try out changes they want to implement in infrastructures or processes to see how the risks and threats might increase or decrease based on emerging trends and predictive analysis that has been done.

Requirement 13: Include Visualization of Trends and Other Situational Awareness Information

Being able to quickly visualize ongoing malicious activity and its impact can reduce analysis time and decrease response time. Finding standard ways to visualize correlated information will be a key to the success of the service. Grégoire discusses visualization for network situational awareness at a local site (Grégoire 2005). The article then goes on to discuss the different types of cognitive processes that require different visualizations: “In many other COPs, different users require different skills to analyze the information presented. Hence, the visualization must support a large number of cognitive processes (perceptions, comprehensions, projections, resolutions) and contexts (management, security, operations).” These ideas need to be taken into account to see what information will be relevant to what roles and how best to display that information.

Requirement 14: Include Different Levels of Information

Different analysts and different types of CSIRTs may require different types of information to be shared. Any service should ensure that information is shared as needed at these different levels.[4] Some may want the raw indicator data, others may want full analysis of the activity, and others may want the trends being seen. How this data will be collected and shared may benefit by including a data architect in the design and implementa-

[4] For more information about mental models, see Floodeen (2013).

tion phases of the project.[5] It is important to think about what actual information participants, CSIRTs in particular, might need. [6] [7] Some may want indicators like IP addresses and domain names, others may want MD5s and file sizes, while others may want descriptions of actors and what type of malicious activity was being performed. Still others may want full blown analysis of attacks including root cause; while others may want developed signatures. The tools and feeds provided by the service should be customizable (as mentioned before) based on the needs and interests of the analysts.

CONSIDERATIONS AND CONSTRAINTS FOR ANY SITUATIONAL AWARENESS TOOLS

For such a service/application to be usable and effective, there are some important considerations that must be addressed. These include but are not limited to the following.

Identification of Standard Metrics and Supporting Metrics Language/Ontology

An important consideration for the Internet Climate and Weather project is the identification and use of a standard set of metrics that have been agreed to for the various data sources to be gathered and made available. Not everyone defines metrics the same way. To be able to logically correlate information, a common understanding and taxonomy would be needed. The CERT Division is currently doing much work in the area of developing ontologies, specifically insider threat indicator ontologies. The work in this area plus working with others in the ontology field would be a good starting point for developing this needed common language.

Confidentiality

Due to the potentially sensitive nature of some information that might be available or sought, any situational awareness service would need some method of sharing confidential or sensitive data. There may have to be non-disclosure agreements and policies in place to ensure that information that is being shared in a secure and confidential manner and is appropriately handled. Also it should be pointed out that collecting multiple types of information across various areas can raise confidentiality issues. Aggregating even open source data can not only concern privacy advocates, but can provide information that could provide malicious actors with greater insight into how to improve their attacks if this information fell into their hands.

Identification of Information Exchange Formats

Besides having standard metrics and supporting taxonomies and ontologies, there will need to be agreement on how information will be collected and exchanged. There are many different data exchange formats in the security arena, and any service will need to choose the ones to support. Providers of such a service may even have to create some type of applications to do format translation where possible.[8]

[5] For information on the phases an analyst goes through to perform situational awareness and to understand how mental models play a part, and therefore to see how the data may need to be fed as part of the service, see D’Amico, Whitley, Tesone, O’Brien, and Roth (2005).

[6] It may be worthwhile to explore how information can be shared in a situational context according to how the attacks moved through the kill chain process. It may give some correlations that can identify precursors for future attacks.

[7] Hutchins, Clopperty, and Amin talk about the Lockheed Martin Kill Chain in the article “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.”

[8] This is also discussed in the conclusion of Grégoire (2005).

Consideration of the Need for a Method for Consistently Anonymizing Shared Data

Depending on how information is collected—by proactive web crawling, collecting network data, or having participants submit information—there may be a need for the data to go through a standard anonymization process before being shared.[9]

Consideration of the need for a voluntary sensor network to collect information

Following the lead of some of the HoneyNet projects, one consideration may be to collect some information by having volunteers host sensors at their location and then having that information correlated and analyzed. This is similar to what CERT.br does with its SpamBot and HoneyPot projects (Hoepers 2012).[10]

Consider Having an Oversight or Advisory Board Made Up of Participating Representatives

Governance of any service is a necessity, as well as ensuring that recipients of the information have a method of providing input to the process and assuring services are provided at a high level of quality.

Based on the Gap Analysis, Determine the Basic Goal and Objectives of the Service

Identify what type of information will be initially collected and the methods that will be used to collect and protect the information. Will information from participant systems and networks be collected? Or will higher level incident information be collected? Or will both be collected, along with analysis, root cause, and other data?

[9] For an example, see Yurcik (2008).

[10] This would be only one type of information collected.

APPENDIX A: EXAMPLES OF TYPES OF DATA CURRENTLY BEING SHARED AND RELATED INFORMATION EXCHANGE PROJECTS OR FORMATS

Internet Storm Center

The Internet Storm Center is a data feed maintained by the SANS Institute. They share information about incidents with subscribers and also the public. Various daily reports are available such as the Top 10 port list, country statistics, and the daily data volume which tracks the number of reports, targets, and sources received.[11]

https://isc.sans.edu/

Team CYMRU

Team CYMRU offers a range of public, restricted, and for-pay services dealing with malware analysis, CSIRT assistance, and the study of the internet's structure. Specifically they will provide "daily lists of compromised or abused devices for the ASNs and/or netblocks with a CSIRT's jurisdiction. This includes such information as bot infected hosts, command and control systems, open resolvers, malware urls, phishing urls, and brute force attacks."[12]

https://www.team-cymru.org/Services/

European Network and Information Security Agency (ENISA)

ENISA provides assistance to European countries who want to start or improve their own CSIRTs. It conducts research and publishes reports on trends and best practices in CSIRT development, implementation, and operation.

http://www.enisa.europa.eu/activities/cert

ENISA also provides excerpts of many of its reports on Pinterest, which is an easy way to display much of its situational awareness results.

https://www.pinterest.com/enisaeu/enisa-reports/

CERT EU

CERT EU offers public information about vulnerabilities, specific threats and incidents, and malware information and attack techniques for European Union organizations.

http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

The Organisation for Economic Co-operation and Development (OECD)

OECD is currently coordinating a project to improve the international comparability of CSIRT statistics.

http://www.oecd.org/fr/sti/ieconomie/informationsecurityandprivacyindicators.htm

Computer Emergency Response Team Brazil (CERT.br)

CERT.br is the Brazilian National CERT. One of their projects is the maintenance of a distributed honeypot network used to improve detection, event correlation, and trend analysis in the Brazilian IP space. The project releases public statistics on network flow data to the honey net as well as hourly port summary statistics. Information is also sent to other CSIRTs about attacks coming from their countries. CERT.br also coordinates a SpamPot network with honey-

[11] Source: https://isc.sans.edu/submissions.html

[12] Source: http://www.team-cymru.org/Services/CAP/

pots in 10 volunteer countries. This network is used to study how spammers attack and use the Internet infrastructure.[13]

http://www.cert.br/projects/

United States Computer Emergency Readiness Team (US-CERT)

US-CERT acts as the United States National CSIRT. They provide alerts on ongoing incidents, vulnerabilities, and best practices for protecting systems, networks, and data.

http://www.us-cert.gov/

Structured Data Languages

MITRE has developed several structured data languages which can be used for communicating cybersecurity data. Today’s automated services require structured data for machine processing and near real-time updates.

http://stix.mitre.org/

Dell SecureWorks

Dell SecureWorks is a managed security service provider whose services include but are not limited to consulting, intelligence, incident response, penetration testing, and PCI compliance. SecureWorks specifically has a Counter Threat Unit, which provides its intelligence services at different levels of subscription. SecureWorks provides news round-ups, global and targeted intelligence reports, and live briefings.[14]

http://www.secureworks.com/

Price Waterhouse Cooper (PWC)

PWC produces the Global State of Information Security Survey, which aims to inform the security community about today’s security challenges.

http://www.pwc.com/gsiss2014

RSA

RSA offers security monitoring and analytics services for enterprise networks, incident management services, and cyber intelligence assessments. They also offer DLP protection options as well as risk and compliance consultations.

http://www.emc.com/security/rsa-security-management.htm

RSA’s parent company, EMC, also offers cybersecurity trending reports.

http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf

http://www.emc.com/resource-library/resource-library.esp

Deloitte

Deloitte offers technical trends information and recommendations for implementing proper cybersecurity management schema.

http://www.deloitte.com/view/en_US/us/Services/consulting/technology-consulting/information-management/index.htm

[13] Source: http://www.cert.br/projects/

[14] Source: http://www.secureworks.com/cyber-threat-intelligence/CTU_intelligence/

Farsight

Farsight security offers a passive DNS database that can be used for investigating DNS entries of others. Farsight hosts this service, but it can be licensed for use in a local network. Farsight also harvests a large amount of other global internet data to provide threat intelligence for their users.

https://www.farsightsecurity.com/Services/

https://www.farsightsecurity.com/Solutions/

Symantec DeepSight

Symantec DeepSight is a security service provider that offers data feeds on several cybersecurity data points, threat intelligence reports, and early warning services. Symantec also creates quarterly threat reports that provide a rough outline of attacks and vulnerabilities seen in a particular time frame.

http://www.symantec.com/deepsight-products

http://www.symantec.com/security_response/publications/threatreport.jsp

Verizon

Verizon produces an annual data breach report detailing a number of security-related metrics, including attack detection speed, sophistication, and attacker prototypes.

http://www.verizonenterprise.com/DBIR/2013/

Ponemon Institute

Ponemon produces a variety of reports studying cyber incidents. These include topics ranging from incident cost and impact studies to the differences between malicious versus non-malicious data breaches. Ponemon also offers consulting services. Ponemon also publishes its well-known *Ponemon Cost of Cybercrime Study*.

http://www.ponemon.org/library

http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

APPENDIX B: BIBLIOGRAPHY

ADS Group. “Summary of ADS Input to the Government’s National CERT Study.” *UK National Computer Emergency Response Team (UK CERT)* (2013). https://www.adsgroup.org.uk/pages/48638552.asp#aGroup_3

D’Amico, Anita & Kocka, Michael. “Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned” 107-112. *Proceedings of the Workshop on Visualization for Computer Security*. Minneapolis, MN, Oct. 2005. IEEE, 2005.

D’Amico, Anita; Whitley, Kirsten; Tesone, Daniel; O’Brien, Brianne; & Roth, Emilie. “Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts,” 229-233. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*, 3 (2005). Orlando, FL, Sep. 2005. Sage, 2005. http://pro.sagepub.com/content/49/3/229

Department of Homeland Security. *National Cyber Incident Response Plan, Interim Version, September 2010.* Department of Homeland Security, 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

Department of Homeland Security. *Privacy Impact Assessment for the National Cybersecurity Protection Program (NCPS) (DHS/NPPD/PIA-026).* Department of Homeland Security, 2012.

Department of Homeland Security. *Situational Awareness Incident Response (SAIR) Tier III Project and Industry Day Notice (Solicitation Number: RFI-OPO-12-0001).* https://www.fbo.gov/index?s=opportunity&mode=form&id=22fdfddc0babb54c0cbc13f751ea5d37&tab=core&_cview=1 (2011).

European Union Agency for Network and Information Security (ENISA). *ENISA ports.* http://www.pinterest.com/enisaeu/enisa-reports/ (2014).

Floodeen, Robert; Haller, John; & Tjaden, Brett. “Identifying a Shared Mental Model Among Incident Responders,”15-25. *2013 Seventh International Conference on IT Security Incident Management and IT Forensics.* Nuremberg, Germany, Mar. 2013. IEEE, 2013. http://www.computer.org/csdl/proceedings/imf/2013/4955/00/4955a015-abs.html

Grégoire, M. & Beaudoin, L. “Visualisation for Network Situational Awareness in Computer Network Defence,” 20-1 – 20-6. *Visualisation and the Common Operational Picture (Meeting Proceedings RTO-MP-IST-043, Paper 20).* RTO, 2005. http://ftp.rta.nato.int/public/pubfulltext/rto/mp/rto-mp-ist-043/mp-ist-043-20.pdf

Haller, John; Carpenter, Jeff; & Allen, Julia. *Establishing a National Computer Security Incident Response Team (CSIRT)* [podcast transcript]. Software Engineering Institute, Carnegie Mellon University, 2010. https://resources.sei.cmu.edu/asset_files/Podcast/2010_016_102_67827.pdf

Haller, John; Merrell, Samuel; Butkovic, Matthew; & Willke, Bradford. *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability* (CMU/SEI-2010-SR-009). Software Engineering Institute, Carnegie Mellon University, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9221

Hoepers, Cristine. “Use of Honeypots for Network Monitoring and Situational Awareness.” *Buenos Aires 2012 FIRST Technical Colloquium.* Buenos Aires, Argentina, Aug. 2012. Brazilian National Computer Emergency Response Team, 2012. http://www.cert.br/docs/palestras/certbr-first-tc2012-1.pdf

Hutchins, Eric M.; Clopperty, Michael J.; & Amin, Rohan M. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” Lockheed tin. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Onwubiko, Cyril & Owens, Thomas. *Situational Awareness in Computer Network Defense: Principles, Methods and Applications (1st ed.).* IGI Publishing, 2012.

Roytman, Michael. “Stop Fixing All the Things – Our BSidesLV Talk.” *The Risk I/O Blog*. http://blog.risk.io/2013/08/stop-fixing-all-the-things-bsideslv/ (2013).

SecureInfo. “SecureInfo to Present at the 6th Annual Computer Emergency Response Team - CERT - Conference, August 3-5, 2004.” *Businesswire*. http://www.businesswire.com/news/home/20040713005838/en/SecureInfo-Present-6th-Annual-Computer-Emergency-Response#.UtmSubROkqV (July 13, 2004).

Skopik, Florian; Bleier, Thomas; & Fiedler, Roman. “Information Management and Sharing for National Cyber Situational Awareness,” 217-227. *ISSE 2012 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference.* Springer Vieweg, 2012. http://www.flosko.at/ait/2012_isse.pdf

Skopik, Florian; Ma, Zhendong; Smith, Paul; & Bleier, Thomas. “Designing a Cyber Attack Information System for National Situational Awareness,” 277-288. *Communications in Computer and Information Science, 318. Future Security: 7th Security Research Conference, Future Security 2012, Bonn, Germany, September 4-6, 2012. Proceedings.* Springer-Verlag, 2012. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.7063&rep=rep1&type=pdf

Yurcik, William; Woolam, Clay; Hellings, Greg; Khan, Latifur; & Thuraisingham, Bhavani. “Safely Sharing Data Between CSIRTs: The SCRUB* Security Anonymization Tool Infrastructure.” *20th Annual FIRST Conference.* Vancouver, British Columbia, Canada, June 2008. http://www.first.org/conference/2008/papers/yurcik-William-slides.pdf

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0000920